

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-222469

(43)Date of publication of application : 21.08.1998

(51)Int.Cl.

G06F 15/00

G06F 19/00

G06T 1/00

(21)Application number : 09-019065

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 31.01.1997

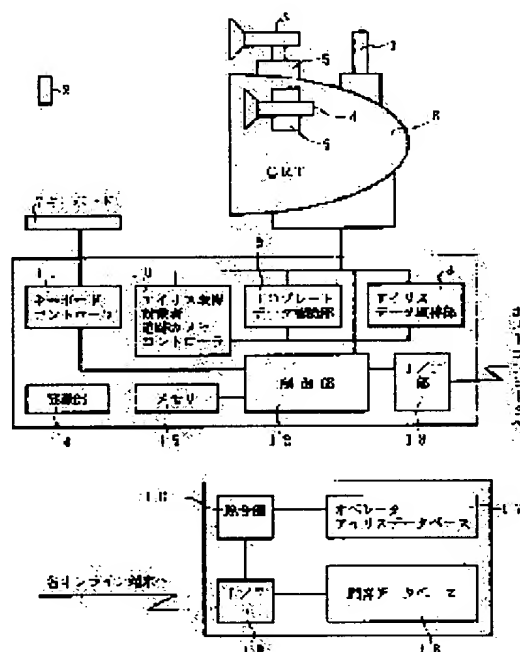
(72)Inventor : NISHIYAMA YASUHIRO

## (54) ON-LINE SYSTEM

## (57)Abstract:

PROBLEM TO BE SOLVED: To prevent the data of host computer from being operated by illegally manipulating a terminal in an on-line system.

SOLUTION: A terminal operator has an ID plate 2 for transmitting ID data, ID data possessed by an ID plate data recognizing part 9 are sent to the host computer by the terminal and collated with ID data stored in an operator iris data base 17 by a collation part 16. When it is judged the possessed ID data show a use permitted operator, iris data possessed by an iris data possessing part 8 are sent to the host computer by the terminal and collated with iris data stored in the operator iris data base 17 by the collation part 16 and when it is judged the possessed iris data shows the use permitted operator, the terminal is turned to a usable state.



[0014] When conducting re-collation, the aforementioned ID data and iris data stored in the memory 15 are sent to the host computer for re-collation at collation unit 16. By not performing re-acquisition of ID data and iris data as described above, it is possible to achieve a higher speed of re-collation processing. When the result of collation at the aforementioned SA 13 or SA 15 is NG, use of the online terminal is disabled, and detection and acquisition of ID data is started again (SA 18).

[0015] To increase strictness of collation, when a prescribed key operation is performed at an enabled terminal, and if iris data acquired again matches with the ID data acquired upon acceptance of the result of collation, the use permission state of the terminal may be maintained by deeming that the bank-clerk having obtained the use permission has started operation. As described above, in the first embodiment of the present invention, when the system of a terminal is started, provision of means for detecting ID data of the ID plate and means for acquiring iris data makes it possible to accomplish automatic online connection without the need for the clerk to be in trouble by the complicated operation such as input of ID card or a password.

[0016] A database which registers ID data and iris data for

all the bank-clerks in the host computer is provided. This makes it possible to enable data operation by an outsider other than the bank-clerks belonging to the bank. Furthermore, there are provided means for detecting transmission wave of the ID plate and means for camera-controlling for making the object iris data acquiring camera and the iris data acquiring camera aiming at an object person. Upon acquiring iris data, this permits acquisition of the iris without being present by the iris data acquiring camera.

[0017] Fig. 3 is a flowchart illustrating a second embodiment of operation, showing the confirming operation during working. In the online-connected terminal, the control unit 12 constantly transmits radio waves from the antenna/scanner 1 (SB 1). Within the reach of an ID plate 2 for radio wave, the ID plate receives wave from the antenna/scanner 1 and terminals ID data (SB 2 and SB 3).

[0018] When receiving of ID data by the antenna/scanner 1 during working steps, the control unit 12 deems the operator to have left the seat, and locks the terminal operation while holding the online connection (SB 9 and SB 5). When the antenna/scanner 1 receives ID data in SB 4, the control unit 12 collates the received ID data with the ID data acquired upon obtaining the use permission and stored in the memory 15 (SB 6). If the result of collation is NG (SB 7), the operator upon obtaining the use permission is deemed to have

been replaced by another, the terminal operation is locked while maintaining the online connection (SB 5).

[0019] If the result of collation at SB 7 is OK, the iris acquisition target follow-up camera control 10 controls the camera controller 5 so that the collimation of the iris data acquisition target follow-up camera 3 and that of the iris data acquiring camera 4 match with the receiver of the ID data. After setting the sights on a target (ID data transmitter) with the iris data acquirer follow-up camera 3 by following up the target, the sights of the iris data acquiring camera 4 are set at eyes of the target, and the image of the eyes is acquired (SB 8 and SB 9).

[0020] The image acquired by the iris data acquiring camera 4 is converted into iris data at the iris data acquiring unit 8 (SB 10). The control unit 12 collates this converted data with the iris data stored in the memory 15 after acquiring upon obtaining a use permission of the terminal (SB 11). When the result of collation is NG (SB 12), the operator is determined to have been replaced by the operator upon obtaining the use permission of terminal, and the terminal operation is locked while holding the online connection (SB 5).

[0021] If the result of collation is OK in the aforementioned SB 12, the terminal is kept in the state of use permission, and when the terminal operation is locked for leaving the operator's seat, lock is released to achieve

a state permitting continuance of operation (SB 13, SB 14). In the second embodiment of the present invention, as described above, the terminal operation can be locked at any time during operation after online connection by detecting and acquiring ID data and iris data, and detecting leaving of the terminal operator from his seat. An illegal use by data operation of the host computer by a person other than the operator upon obtaining the use permission of the terminal can thus be prevented.

[0022] Locking is released when the operator upon obtaining the use permission of the terminal comes back to his seat and the ID data and the iris data can thus be obtained, thus enabling to minimize troubles in reactivation. In addition, by storing and holding the ID data and the iris data acquired upon obtaining the use permission of the terminal, collation can be performed without accessing the host computer, thereby permitting achievement of the higher speed of processing.

[0023] In the first embodiment and the second embodiment described above, a bank online system has been described above. The present invention is applicable also in public agencies and the like using an online system handling important information.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-222469

(43) 公開日 平成10年(1998) 8月21日

(51) Int.Cl.<sup>8</sup>

G 0 6 F 15/00

19/00

G 0 6 T 1/00

識別記号

3 3 0

F I

G 0 6 F 15/00

15/30

15/64

3 3 0 F

3 3 0

H

審査請求 未請求 請求項の数6 O L (全 7 頁)

(21) 出願番号

特願平9-19065

(22) 出願日

平成9年(1997) 1月31日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 西山 康弘

東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

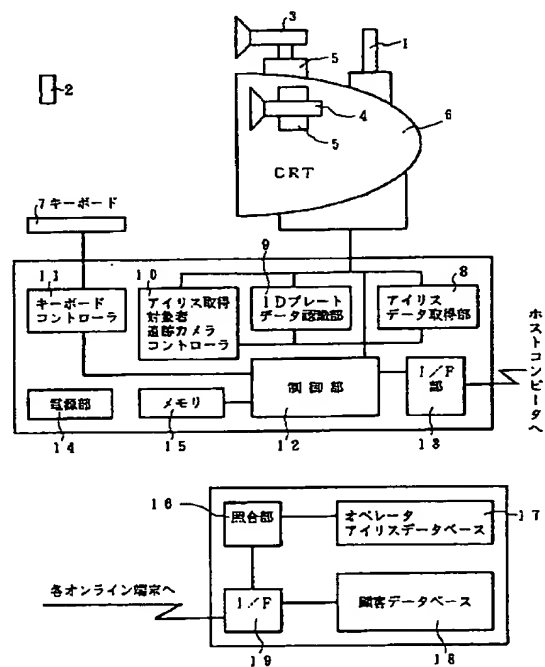
(74) 代理人 弁理士 大西 健治

(54) 【発明の名称】 オンラインシステム

(57) 【要約】

【課題】 オンラインシステムにおいて、不正に端末を操作してホストコンピュータのデータを操作できないようにする。

【解決手段】 端末操作者は、IDデータを発信するIDプレート2を持ち、端末は、IDプレートデータ認識部9で取得したIDデータをホストコンピュータに送り、照合部16でオペレータアイリスデータベース17に記憶してあるIDデータと照合して、取得したIDデータが使用を許可した操作者のものであると判断すると、端末はアイリスデータ取得部8で取得したアイリスデータをホストコンピュータに送り、照合部16でオペレータアイリスデータベース17に記憶してあるアイリスデータと照合して、取得したアイリスデータが使用を許可した操作者のものであると判断すると、端末を使用可能状態とする。



本発明のオンラインシステムの実施の形態の一例を示すブロック図

**【特許請求の範囲】**

**【請求項 1】** ホストコンピュータに複数の端末を接続し、使用が許可された端末操作者を識別して、該当する端末を使用可能とするオンラインシステムにおいて、前記端末操作者は、当該操作者に割り当てられた ID データを発信する ID プレートを持ち、前記端末は、前記 ID プレートから発信される ID データを受信する手段と、端末操作者の画像を取得するカメラと、前記カメラで取得した画像からアイリスデータを取得する手段とを備え、前記ホストコンピュータは、使用が許可された複数の端末操作者の ID データとアイリスデータを記憶しておく手段を備え、

ID プレートから取得した ID データとホストコンピュータで管理している ID データとを照合して、該 ID プレートから取得した ID データが使用を許可された端末操作者のものであると判断すると、この使用が許可されている ID データを発信した ID プレートを所持する端末操作者の画像から取得したアイリスデータとホストコンピュータで管理しているアイリスデータとを照合して、取得したアイリスデータが使用を許可された端末操作者のものであると判断すると、該当する端末を使用可能とすることを特徴とするオンラインシステム。

**【請求項 2】** 請求項 1 記載のオンラインシステムにおいて、前記端末に、該端末を使用可能とした後、最初に操作が実行された時に、再度アイリスデータを取得する手段と、取得したアイリスデータが使用を許可された端末操作者のものでない判断すると、端末の使用を不可能とすることを特徴とするオンラインシステム。

**【請求項 3】** 請求項 1 または 2 記載のオンラインシステムにおいて、前記 ID データおよびアイリスデータの照合は、ホストコンピュータで行うことを特徴とするオンラインシステム。

**【請求項 4】** 請求項 1、2 または 3 記載のオンラインシステムにおいて、前記端末に、前記 ID プレートから発信される ID データの到来方向を検知する手段と、前記カメラを ID データの到来方向に向ける手段とを備えたことを特徴とするオンラインシステム。

**【請求項 5】** 請求項 1、2、3 または 4 記載のオンラインシステムにおいて、前記端末に、該端末を使用可能とした際に取得した ID データおよびアイリスデータを記憶する手段と、ID データを継続して受信する手段と、前記受信手段で取得した ID データと前記記憶した ID データを照合し、正当性を判断するとこの正当であると

判断された ID データを発信した ID プレートを所持する操作端末者の画像からアイリスデータを取得し、この取得したアイリスデータと前記記憶したアイリスデータを照合し、正当性を判断すると該当端末を使用可能とし、ID データとアイリスデータの少なくとも一方でも正当性を判断できない場合は、該当端末を使用不可能とする手段を備えたことを特徴とするオンラインシステム。

**【請求項 6】** 請求項 5 記載のオンラインシステムにおいて、前記端末に、ID データの受信の有無を判断する手段と、ID データを受信しなくなったと判断すると、該当端末を使用不可能とする手段を備えたことを特徴とするオンラインシステム。

**【発明の詳細な説明】****【0001】**

**【発明の属する技術分野】** 本発明は、銀行等に構築されるオンラインシステムにおいて、端末装置の使用に対するセキュリティに関するものである。

**【0002】**

**【従来の技術】** 従来、この種のオンライン端末装置は、オペレータが地区センタ等のホストコンピュータにオンライン接続する際、カードリーダーにオペレータ自身の ID カードを通し、キーボードからパスワードを入力する。地区センタ等のホストコンピュータは、そのデータを照合して OK ならばオンライン接続許可を行い、オペレータはオンライン端末を使用して業務を行う。

**【0003】**

**【発明が解決しようとする課題】** しかしながら、ID カードの紛失、盗難や偽造、パスワードの漏洩によって部外者によるオンライン接続が可能であり、オンライン端末を使用し、ホストコンピュータ上のデータを操作される可能性があるという問題がある。また、オペレータが離席する場合、オンライン端末はオペレータ自身の ID でオンライン接続されたまま放置されている場合が多く、オペレータ以外の部外者が使用できる可能性があるという問題がある。

**【0004】**

**【課題を解決するための手段】** 上述した課題を解決するため、本発明は、ホストコンピュータに複数の端末を接続し、使用が許可された端末操作者を識別して、該当する端末を使用可能とするオンラインシステムにおいて、前記端末操作者は、当該操作者に割り当てられた ID データを発信する ID プレートを持ち、前記端末は、前記 ID プレートから発信される ID データを受信する手段と、端末操作者の画像を取得するカメラと、前記カメラで取得した画像からアイリスデータを取得する手段とを備え、前記ホストコンピュータは、使用が許可された複数の端末操作者の ID データとアイリスデータを記憶し

ておく手段を備え、IDプレートから取得したIDデータとホストコンピュータで管理しているIDデータとを照合して、該IDプレートから取得したIDデータが使用を許可された端末操作者のものであると判断すると、この使用が許可されているIDデータを発信したIDプレートを所持する端末操作者の画像から取得したアイリスデータとホストコンピュータで管理しているアイリスデータとを照合して、取得したアイリスデータが使用を許可された端末操作者のものであると判断すると、該当する端末を使用可能とすることとしたものである。

#### 【0005】

【発明の実施の形態】図1は本発明のオンラインシステムの実施の形態の一例を示すブロック図である。図において、1はアンテナ／スキャナ、2はIDプレートで、このIDプレート2は、前記アンテナ／スキャナ1から放射される電波に反応し、エコー波を発信する機能を埋め込んだ無線式のネームプレートで、アンテナ／スキャナ1は、上述したようにIDプレート2から発信されるエコー波を検出する。

【0006】3は虹彩取得対象者追跡用カメラ、4は虹彩データ取得用カメラ、5は虹彩データ取得対象者にカメラの照準を合わせるためのカメラコントローラ、6はCRT、7はキーボード、8は前記虹彩データ取得用カメラ4より取得した画像を虹彩データに変換し、制御部12にデータを送出するアイリスデータ取得部、9は前記アンテナ／スキャナ1が受信したIDプレート情報をデータに変換し、制御部12にデータを送出するIDプレートデータ認識部、10はIDプレート2を所持または着衣に付けている対象者に前記虹彩データ取得対象者追跡用カメラ3と虹彩データ取得用カメラ4の照準を合わせるよう各カメラをコントロールするアイリス取得対象者追跡カメラコントローラ、11はオペレータが離席した場合にオンライン端末の操作をロックさせるためのキーボードコントローラである。上述した制御部12は、各部からのデータを受け、該制御部12とホストコンピュータのデータを送受信を行うためのI/F部13を介してホストコンピュータへのデータの送受信を行い、各コントローラへのコントロール指示を行う。

【0007】14は各部へ電源供給するための電源、15はオンライン接続許可時のIDデータと虹彩データを保持するためのメモリである。16はオンライン端末から受信した虹彩データとオペレータアイリスデータベース17とを照合する照合部で、前記オペレータアイリスデータベース17には、オペレータの登録IDデータおよび登録アイリスデータが保管してある。

【0008】18は業務に関する顧客データを保管してある顧客データベース、19は各オンライン端末とのデータの送受信を行うためのI/F部である。次に、図1で説明したオンラインシステムの動作を、ここではオンライン端末を使用している銀行を例に説明する。図2は

動作の第1の実施の形態を示すフローチャートで、システム立ち上げから業務開始までの動作を示す。

【0009】銀行の行員全員のユニフォームの胸に、各行員毎に割り当てたエコー波を発信するIDプレート2を付けている。行員は、業務開始時にオンライン接続をするためにオンライン端末の電源をONする。システムが立ち上がると、アンテナ／スキャナ1から電波が発信され、IDプレート2がその電波を検出すると、該IDプレート2はIDデータを発信する(SA1~SA4)。

【0010】アンテナ／スキャナ1は、そのIDデータを受信すると、IDプレートデータ認識部9へ送出する。IDプレートデータ認識部9は、制御部12およびI/F部13を介し、ホストコンピュータにIDデータを送出する(SA5, SA6)。ホストコンピュータは、受信したIDデータと登録されているIDデータを照合し、オンライン端末使用許可対象者が否かを認識し、その照合結果をオンライン端末に発信する(SA7, SA8)。

【0011】アンテナ／スキャナ1は常に電波を発信し、照合結果がNGの場合、再度IDデータの受信および照合を繰り返す。照合結果がOKの場合、虹彩データ取得対象者追跡用カメラ3および虹彩データ取得用カメラ4の照準がIDデータの受信対象者に合うように、アイリス取得対象者追跡カメラコントロール10はカメラコントローラ5をコントロールし、まず、虹彩データ取得対象者追跡用カメラ3で対象者(IDデータ発信者)を追跡して該対象者に照準を合わせた後、虹彩データ取得用カメラ4の照準を対象者の目に合わせ、目の画像を取得する(SA9, SA10)。ここで、虹彩データ取得対象者追跡用カメラ3および虹彩データ取得用カメラ4で対象者(IDデータ発信者)を追跡するため、アイリス取得対象者追跡カメラコントロール10は、IDデータの到来方向を検知し、このIDデータが到来する方向に虹彩データ取得対象者追跡用カメラ3および虹彩データ取得用カメラ4を向けるようにする。例えば、アンテナ／スキャナ1を動かした際の電波の強弱の変化からIDデータの到来方向を検知したり、複数のアンテナを設けて各アンテナの出力差からIDデータの到来方向を検知することが可能である。

【0012】虹彩データ取得用カメラ4によって取得された画像はアイリスデータ取得部8でアイリスデータに変換し、そのデータを制御部12およびI/F部13を介してホストコンピュータのI/F部18へ送る(SA11)。ホストコンピュータのI/F部18は、受信したアイリスデータを照合部16に送る。照合部16は、受信したアイリスデータとオペレータアイリスデータベース17に登録されているデータとを照合し、照合結果をオンライン端末へ発信する(SA12, SA13)。

【0013】照合結果がOKの場合は、オンライン端末



の使用を許可し、許可時に取得したIDデータとアイリスデータをメモリ15に記憶する(SA14, SA15)。なお、この状態で業務を開始可能状態としてもよいが、照合の誤りで端末の使用許可を出すことがないように、再度照合を行い、照合結果がOKであれば、業務を開始可能状態とすることで、偶然による端末使用の許可を防ぐ(SA16, SA17)。

【0014】再度照合を行う場合、メモリ15に記憶した前記IDデータとアイリスデータをホストコンピュータに送り、照合部16で再照合を行う。このように、IDデータおよびアイリスデータの再取得を行わないことで、再照合の処理を高速にできる。前記SA13あるいはSA16で照合結果がNGの場合は、オンライン端末の使用を不許可とし、再度IDデータの検出、取得から行う(SA18)。

【0015】また、照合の厳密性を増すため、使用が許可された端末において、所定のキー操作がなされると、再度アイリスデータを取得して、照合の結果許可時に取得したIDデータと一致すれば、使用を許可した行員が操作を開始したものと、端末の使用可能状態を保持するようにしてもよい。以上説明したように、本発明の第1の実施の形態では、端末のシステムが立ち上がると、IDプレートのIDデータを検出する手段と、アイリスデータを取得する手段を設けたことで、行員がIDカードやパスワード入力といった煩わしい操作をすることなく、自動でオンライン接続をすることができる。

【0016】また、ホストコンピュータには全行の行員のIDデータとアイリスデータを登録するデータベースを設けたことで、その支店に所属する行員以外の部外者によるデータ操作を不可能にすることができる。さらに、IDプレートの発信電波を検出する手段と対象者虹彩データ取得用カメラと虹彩データ取得用カメラの照準を対象者に合わせるためのカメラコントロールをする手段を設けたので、虹彩データ取得の際、虹彩データ取得用カメラの前に居ることなく虹彩を取得できる。

【0017】図3は動作の第2の実施の形態を示すフローチャートで、業務中の確認動作を示す。オンライン接続された端末において、制御部12はアンテナ/スキャナ1から常に電波を発信する(SB1)。IDプレート2が電波の到達範囲内にあれば、該IDプレート2はアンテナ/スキャナ1からの電波を受信し、IDデータを発信する(SB2, SB3)。

【0018】制御部12は業務中にアンテナ/スキャナ1でIDデータを受信しなくなると、操作者が離席したものと判断して、オンライン接続は保持したまま、端末操作をロックする(SB4, SB5)。前記SB4でアンテナ/スキャナ1がIDデータを受信すると、この受信したIDデータと、端末使用許可時に取得してメモリ15に記憶しておいたIDデータを照合する(SB6)。照合結果がNGであると(SB7)、操作者が端

末使用許可時の操作者と変わったものと判断して、オンライン接続は保持したまま、端末操作をロックする(SB5)。

【0019】前記SB7で照合結果がOKであると、虹彩データ取得対象者追跡用カメラ3および虹彩データ取得用カメラ4の照準がIDデータの受信対象者に合うように、アイリス取得対象者追跡カメラコントロール10はカメラコントローラ5をコントロールし、まず、虹彩データ取得対象者追跡用カメラ3で対象者(IDデータ発信者)を追跡して該対象者に照準を合わせた後、虹彩データ取得用カメラ4の照準を対象者の目に合わせ、目の画像を取得する(SB8, SB9)。

【0020】虹彩データ取得用カメラ4によって取得された画像はアイリスデータ取得部8でアイリスデータに変換し(SB10)、制御部12は、この変換したデータと、端末使用許可時に取得してメモリ15に記憶しておいたアイリスデータを照合する(SB11)。照合結果がNGであると(SB12)、操作者が端末使用許可時の操作者と変わったものと判断して、オンライン接続は保持したまま、端末操作をロックする(SB5)。

【0021】前記SB12で照合結果がOKであると、継続して端末を使用許可状態とし、離席等で端末操作がロックされている場合は、ロックを解除して、業務が継続可能な状態となる(SB13, SB14)。以上説明したように、本発明の第2の実施の形態では、オンライン接続後の業務中に、常にIDデータとアイリスデータを検出および取得し、端末操作者の離席を検知することにより端末操作をロックでき、端末使用許可時の操作者以外の人物によるホストコンピュータのデータ操作による不正を防ぐことができる。

【0022】また、端末使用許可時の操作者が戻ってくること、該操作者のIDデータとアイリスデータが取得できれば、ロックが解除されるので、再立ち上げの手間を省くことができる。さらに、端末使用許可時に取得したIDデータとアイリスデータを端末内のメモリに記憶して保持しておくことにより、ホストコンピュータへのアクセス無しに照合が行え、処理時間を高速にできる。

【0023】なお、上述した第1の実施の形態および第2の実施の形態では、銀行のオンラインシステムについて説明したが、重要情報を取り扱うオンラインシステムを使用している官公庁等の機関においても用いることができる。

【0024】

【発明の効果】以上説明したように、本発明は、端末操作者は、当該操作者に割り当てられたIDデータを発信するIDプレートを持ち、端末ではIDデータを取得すると、この取得したIDデータが使用を許可されている操作者のものであるか否かを判断し、取得したIDデータが使用を許可されている操作者のものであると判断す

IDの予-照合を行い

IDが受信できるとは、メモリ15に記憶

[Fig. 1]

7: KEYBOARD

11: KEYBOARD CONTROLLER

10: IRIS ACQUIRER FOLLOW-UP CAMERA

9: ID PLATE DATA RECOGNITION UNIT

8: IRIS DATA ACQUIRING UNIT

14: POWER SUPPLY

15: MEMORY

12: CONTROLLING UNIT

13: I/F UNIT

① TO HOST COMPUTER

② TO INDIVIDUAL ONLINE TERMINALS

16: COLLATION UNIT

17: IOERATIR'S URUS DATABASE

18: CUSTOMER DATABASE

BLOCK DIAGRAM ILLUSTRATING A TYPICAL EMBODIMENT OF THE  
ONLINE SYSTEM OF THE PRESENT INVENTION

ると、このIDデータを発信している操作者のアイリスデータを取得して、この取得したアイリスデータが使用を許可されている操作者のものであるか否かを判断し、取得したアイリスデータが使用を許可されている操作者のものであると判断すると、該当端末を使用可能とすることとしたので、端末操作者がIDカードやパスワード入力といった煩わしい操作をすることなく、自動でオンライン接続をすることができる。

【0025】また、使用を許可した全操作者のIDデータとアイリスデータを登録したデータベースを備え、端末で取得したIDデータおよびアイリスデータをこのデータベースを用いて照合することで、部外者によるデータ操作を不可能にすることができる。さらに、照合に操作者から取得したアイリスデータを用いることで、盗難や偽造等によるデータの作成が不可能となり、照合の厳密性を増すことが可能となる。

# 【図面の簡単な説明】

【図1】本発明のオンラインシステムの実施の形態の一例を示すブロック図

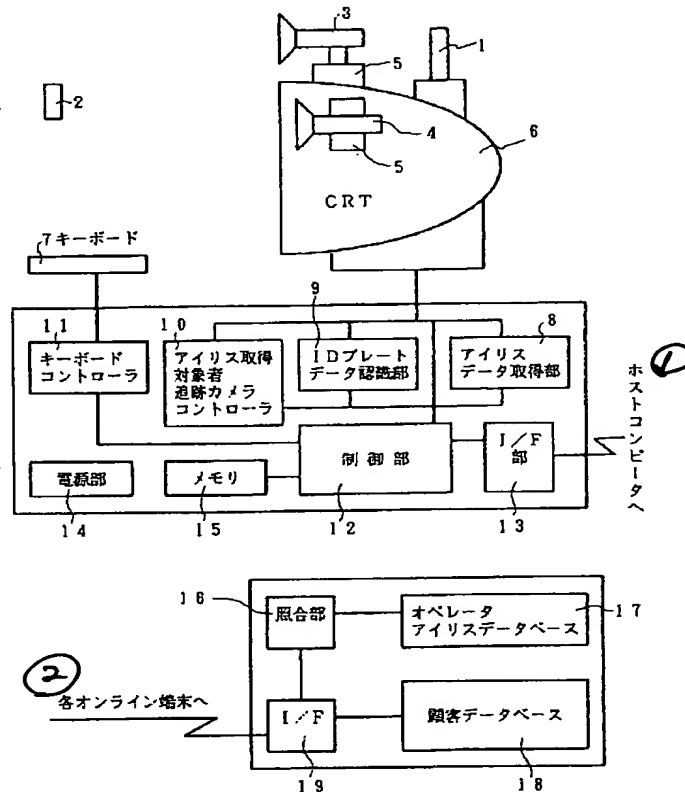
【図2】動作の第1の実施の形態を示すフローチャート

【図3】動作の第2の実施の形態を示すフローチャート

## 【符号の説明】

- 1 アンテナ／スキャナ
- 2 IDプレート
- 4 虹彩データ取得用カメラ
- 7 キーボード
- 8 アイリスデータ取得部
- 9 IDプレートデータ認識部
- 12 制御部
- 16 照合部
- 17 オペレータアイリスデータベース
- 18 顧客データベース

【図1】



本発明のオンラインシステムの実施の形態の一例を示すブロック図

[FIG. 2]

① ONLINE TERMINAL POWER SUPPLY OK

SA 1:      ACTIVATE SYSTEM

SA 2:      TRANSMIT WAVE FROM ANTENNA/SCANNER

SA 3:      RECEIVE ID PLATE RADIO WAVE

SA 4:      TRANSMIT ID PLATE ID DATA

SA 5:      RECEIVE ANTENNA/SCANNER ID DATA

SA 6:      TRANSMIT ID DATA TO HOST COMPUTER

SA 7:      COLLATE RECEIVED DATA WITH REGISTERED DATA, AND  
            TRANSMIT RESULT TO ONLINE TERMINAL

SA 8:      RESULT OF COLLATION

SA 9:      CONTROL CAMERA SO AS TO AIM AT COLLATED ID PLATE  
            HOLDER

SA 10:     COLLIMATE CAMERA

SA 11:     CONVERT DATA INTO IRIS DATA AND TRANSMIT IT TO HOST  
            COMPUTER

SA 12:     COLLATE IRIS DATA WITH REGISTERED DATA, AND  
            TRANSMIT THE RESULT TO ONLINE TERMINAL

SA 13:     RESULT OF COLLATION

SA 14:     USE PERMISSION OF ONLINE TERMINAL

SA 15:     ONLINE TERMINAL HOLDS ID DATA AND IRIS DATA FOR  
            WHICH USE PERMISSION HAS BEEN OBTAINED

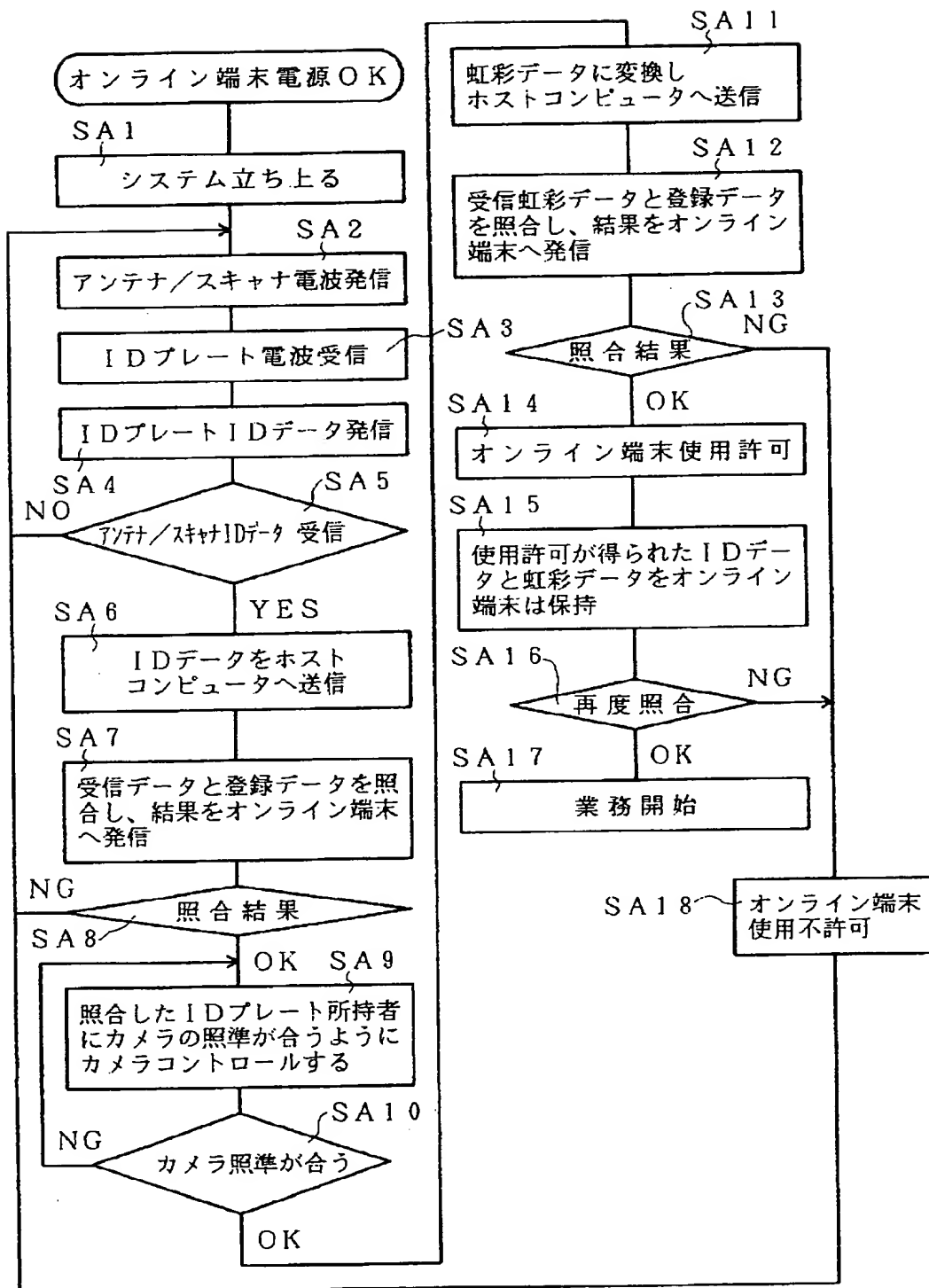
SA 16:     RE-COLLATE DATA

SA 17:     START OPERATION

SA 18:     NOT GRANTING USE PERMISSION OF ONLINE TERMINAL

FLOWCHART SHOWING FIRST EMBODIMENT OF OPERATION

【図2】



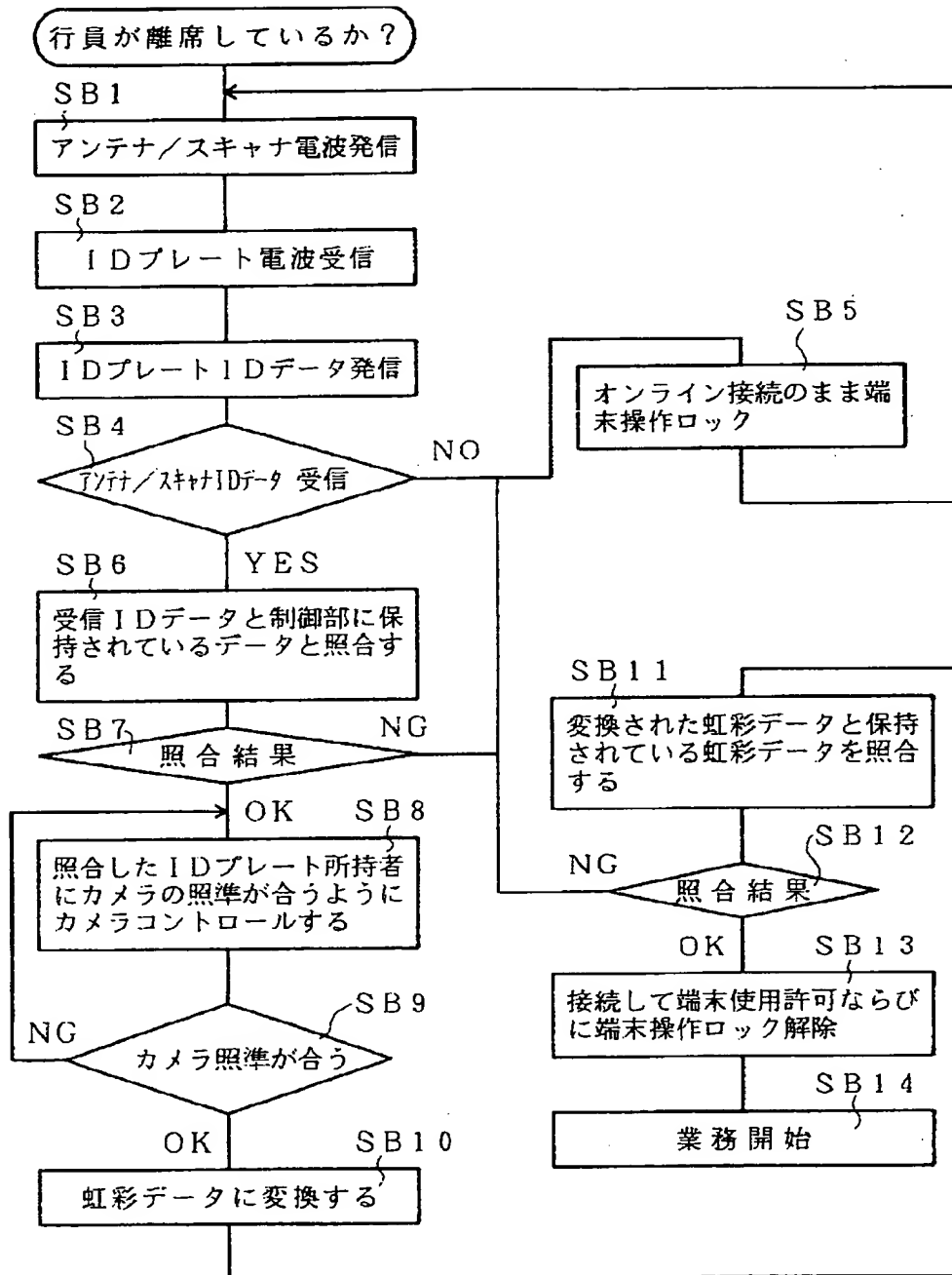
動作の第1の実施の形態を示すフローチャート

[FIG. 3]

- ① IS BANK-CLERK ABSENT FROM THIS SEAT?
- SB 1: TRANSMIT RADIO WAVE FROM ANTENNA/SCANNER
- SB 2: RECEIVE RADIO WAVE OF ID PLATE
- SB 3: TRANSMIT ID PLATE ID DATA
- SB 4: RECEIVE ANTENNA/SCANNER ID DATA
- SB 5: LOCK TERMINAL OPERATION WHILE HOLDING ONLINE  
CONNECTION
- SB 6: COLLATE RECEIVED ID DATA WITH DATA HELD IN CONTROL  
UNIT
- SB 7: RESULT OF COLLATION
- SB 8: CONTROL CAMERA SO AS TO AIM AT HOLDER OF COLLATED  
ID PLATE
- SB 9: COLLIMATE CAMERA
- SB 10: CONVERT DATA INTO IRIS DATA
- SB 11: COLLATE CONVERTED IRIS DATA WITH STORED IRIS DATA
- SB 12: RESULT OF COLLATION
- SB 13: CONVERT, AND GRANT USE PERMISSION OF TERMINAL AND  
RELEASE LOCKING OF TERMINAL OPERATION
- SB 14: START OPERATION

FLOWCHART SHOWING SECOND EMBODIMENT OF OPERATION

【図3】



動作の第2の実施の形態を示すフローチャート

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-269183

(43)Date of publication of application : 09.10.1998

(51)Int.Cl.

G06F 15/00

G06F 19/00

G06T 7/00

(21)Application number : 09-076152

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 27.03.1997

(72)Inventor : NISHIYAMA TADASHI  
SUTANI MASASHI(54) AUTOMATIC TRANSACTION DEVICE, AUTOMATIC TRANSACTION DEVICE SYSTEM,  
AND IRIS PATTERN REGISTERING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance the safety of an individual recognition processing.

SOLUTION: A card read part 12 reads the iris pattern of the owner of a card from the card C and delivers it to a collation part 13 and an iris feature extraction part 11 extracts the iris pattern of a customer from video images fetched by a camera 10 and delivers it to the collation part 13. The collation part 13 collates the iris pattern of the card owner with the iris pattern of the customer, obtains a matching degree between both iris patterns and delivers it to a transaction control part 14. The transaction control part 14 judges whether or not the customer is the card owner from the matching degree between both iris patterns, and when the customer is the card owner, instructs the customer to input a password number from an operation panel 7 and performs individual recognition with the password number.

